Doc Code: AP.PRE.REQ

PTO/SB/33 (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 915-008.020

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on May 18, 2009

Signature Marilyn O'Connell

Typed or printed name Marilyn O'Connell

Application Number	Filed
10/771,836	Feb. 3, 2004

First Named Inventor: Lauri PAATERO

Art Unit	Examiner
2431	Shin Hon Chen

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [x] attorney or agent of record. Registration number 31,391
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Francis Maguire
Signature

Francis J. Maguire
Typed or printed name

(203) 261-1234
Telephone number

May 18, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [ ] *Total of _____ forms are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re Application of: Lauri PAATERO

Serial No.: 10/771,836 Art Unit: 2431

Filed: February 3, 2004 Examiner: Shin Hon Chen

Docket Number: 915-008.020

For: ARCHITECTURE FOR ENCRYPTED APPLICATION INSTALLATION

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

ACCOMPANIED BY NOTICE OF APPEAL

Sir:

In response to the Final Action of February 17, 2009, Applicant requests review of the rejection prior to preparing an Appeal Brief for the following reasons:

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Mark O'Connell
Marilyn O'Connell

Dated: May 18, 2009

REMARKS

Regarding the subject matter of independent method claim 1, it can be understood by viewing the claim alongside Fig. 2. In Fig. 2, a secure channel 207 is shown connecting a server 208 to an installation part 203 of an application 202 and connecting the installation part 203 to a secure environment 205 in the device 201. The device 201 may be a terminal device as claimed in claim 1 and receive a first key in its secure environment 205 via the secure channel 207 from the server 208 outside the terminal 201. The first key is for decrypting an encrypted application 204. The secure channel 207 may for example (as discussed in the specification) involve the server 208 encrypting the first key with a public key of device 201. It is also possible to for instance use the SSL protocol to transfer the first key into the secure environment 205. See page 3, paragraph 0028 in the right-hand column at lines 14-23. The protected (encrypted) application part 204 is then decrypted in the secure environment 205 by means of the first key (which came from the server). Before being stored back outside the secure environment, the application is re-encrypted in the secure environment by means of a second key.

In Section 4 beginning on page 2 of the Detailed Action, the Examiner refers to *Cassagnol* for disclosing the receiving in a secure environment in a terminal via a secure channel from a server outside the terminal a first key for decrypting an encrypted application, pointing to paragraphs [0109]-[0112]. These paragraphs cover the first two steps shown in Fig. 6 of *Cassagnol*. In those steps, the test jig 122 with the adapter 10 uses the public key of the server 120 to encrypt a triple DES session key which it then sends to the server 120 via the network 128. The key server decrypts the triple key generated in the test jig using its private key so as to access the session key. The key server then sends the apparatus 10 some random numbers from the key server's source 126 to update the seed material on the apparatus 10. It will also send any assigned configuration, such as a serial number, and a software export/import master key (MK). This is shown in the second arrow in Fig. 6 going from right to left and labeled DES (Config). This is presumably encrypted with the session key received from the test jig 122. The remaining part of

Fig. 6 also has to do with the generation, encryption and reprogramming of the EEPROM 32 of Fig. 3 which is the repository of the key material (see page 8 at paragraph [0071] and page 9 at paragraph [0086]). Notice that there is nothing discussed here about decryption or re-encryption of an application part such as the application part 204 of Fig. 2 of the present disclosure. In other words, the statement by the Examiner that the first key is for decrypting an encrypted application does not seem to correspond to what is shown in Figs. 5 and 6 of *Cassagnol* which seem to deal with key management.

The Examiner seems to recognize this fact by reference to paragraph [0025] of *Cassagnol* which the Examiner asserts discloses decrypting, in the secure environment, the encrypted application by means of the first key, pointing to the whitening key disclosed in paragraph 0025. However, this whitening key is not sent by the key server in Fig. 5 or 6 but rather is generated by the adapter 10 itself.

The Examiner goes on to analogize the re-encrypting in the secure environment to this same whitening key. The Examiner confirmed to the undersigned that he is referring to the MK key which, as explained above, is shown in the second arrow of Fig. 6 being transferred from the key server 120 to the test jig 122. But the citation at [0025] does not refer to using any such first key to decrypt an encrypted application as claimed in claim 1. So, it seems that the Examiner's analysis is missing this crucial aspect of the claim where it is stated that the encrypted application is decrypted by means of the first key. This is clear error.

The presently claimed first key and the software export/import master key MK in paragraph [0112] of *Cassagnol* are not the same. In *Cassagnol* the whitening processes are performed by the cipher means, which comprises a crypto module 20 (see Fig. 3) which is capable of performing triple key encryption and decryption with whitening etc. [0048, 0056]. The encryption/decryption key is employed by the cipher means are protected utilizing a key hierarchy. The triple DES process is keyed with the session key. To obtain the session key one must have the master key, and to obtain the master key access to the device key is required [0061]. Further, in the same paragraph [0061] it is stated that unencrypted versions of the session key, the master key, and the device key are only available in the cipherer 20 and the

cipherer's key facility. Further still, in paragraphs [0110]-[0112], the communication process between the device and the server as shown in Fig. 6 is described as one in which the device first creates a new random seed which is then used to create a session key. To obtain the session key one must have the master key, and to obtain the master key access to the device key is required. This is all done within the device. In other words, a master key is employed in the device. The session key is then encrypted with the public key of the key server and is sent to the key server, which session key is then decrypted with the private key of the server and utilized for any further communication between the device and the server. Thereafter, an export/import master key (MK) is sent to the test jig. Still further, in [0085] it is stated that the generation of *whitening keys* is obtained by utilizing an entropy source 408, the CSPRNG and further in [0086] the route key (device key) for the key hierarchy is loaded via the key isolation circuit. (This is shown only as a signal line in Fig. 3.) To ensure the keys cannot be accessed ... the memory 32, the logic circuit 34, the key isolation circuit 50 and the crypto module 20 define a *closed system.*

Further, in the Response to Arguments on page 15, paragraph 40, of the Office Action it is stated that the import/export master key is transferred from the key server to the apparatus and the whitening key is later generated through different cycles of import/export following the initial import/export key operation discloses that the first key is the import/export master key and whitening key in the key cycling process, i.e. alleging that the import/export master key and whitening key together would form the first key of the present claim 1. Applicant respectfully disagrees since the whitening key is generated in the device. From paragraph [0085] it is shown that the whitening keys are not based in any way on the import /export master key, but rather on the generation of a pseudo-number. Thus the whitening key is not received from the outside of the device. Nor is any information that is used to generate the whitening key.

From the foregoing, it appears that the term master key is used in a very unclear way in the document and it is not clear from the document nor is it explicitly shown how this export/import MK is used. In fact, it is emphasized in [0104, 0105]

that is more secure to generate keys within the device by self-keying. If it can be shown that the export/import master key is indeed used to obtain the first key, being the first whitening key, by the crypto module utilizing the key hierarchy as described above, it is at least true that the export/import MK is not equal to the first key according to the present invention. Thus, the present inventive concept of receiving the first key to decrypt an encrypted application via a secure channel is not shown in *Cassagnol* which, on the contrary, supports self-keying and generation of any keys within the device. Therefore, for at least this reason claim 1 is not disclosed or suggested by the cited references.

With regard to independent claim 2, it again has not been shown explicitly in the *Cassagnol* reference where the first key that is for decrypting an encrypted application is encrypted by means of a second key and stored outside the secure environment. The passage at paragraph 0058 of *Cassagnol* does not seem to disclose anything like that. It does discuss an encrypted version of the whitening key but that is not the same thing as the first key received from the key server 120.

Regarding claims 8, 9, 22 and 24, the same comments apply as made above apply as well.

For these reasons as well the novelty rejection is in clear error.

All of the claims rejected on the ground of Section 103 are nonobvious for at least the same reasons as given above in applicant overcoming the novelty rejection.

Reopening of prosecution and allowance is requested.

Respectfully submitted,

Francis J. Maguire
Registration No. 31,391
Attorney for the Applicant

FJM/mo
Ware, Fressola, Van Der Sluys & Adolphson LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468
(203) 261-1234